

Any Buyer Accepted

Unregulated data markets create personal security risks, including scams and foreign interference



Summary

Summary

The way data is collected and used for most advertising online – called the Real-Time Bidding (RTB) process – sees deeply sensitive data about Australians shown to and shared with unknown parties thousands of times a day. Through RTB, foreign states and nefarious actors can collect massive data hauls on everyday Australians.

- Sensitive data about Australians is broadcast widely in a free-for-all manner each and every day:
 - The RTB system broadcasts where a person in Australia is 449 times a day to an unknown, and uncontrolled number of companies.
 - One dataset alone – the Australian Eyeota (Dun & Bradstreet) data – shows 17,501 unique data categories being broadcast.

This creates risks of:

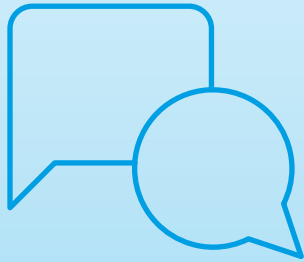
- Scams: There are no effective controls on who can see or access this data, meaning it is readily available to nefarious actors, such as scammers. This report documents the trading of data about people likely to have used toll booths, which can be used to personalise scam messages about ‘fake road tolls’. It also documents the trading of data about people likely to be expecting a parcel, which can be used to personalise fake ‘Australia Post’ parcel delivery scams, for example.
- Foreign interference: Google and other RTB firms send RTB data about Australians to Chinese and Russian firms, where national laws enable security agencies to access the data.
- We urgently need reforms to the *Privacy Act* to protect Australians from these unnecessary risks, which are beyond the control of individuals to manage. Even if people use secure devices, data will still flow via RTB from personal devices, friends, family, and personal contacts. Stronger data protections to regulate the flow of this information is required.
- We also note other elements in the Government’s regulatory pipeline are relevant – namely the Scams Prevention Framework and the statutory review of the *Online Safety Act 2021*. These valuable, necessary interventions do not account for the creation and marketisation of personal data that creates foreseeable personal security risks. Proactive obligations need to be placed on data collecting and data trading firms to exercise fairness and reasonableness in the collection of personal data.

This report builds on the evidence and analysis from the Irish Council of Civil Liberties (ICCL), who released a compelling report—*Australia’s Hidden Security Crisis*¹—documenting how the RTB process creates national security risks resulting from the widespread broadcasting of data about Australian military personnel and security staff. The widespread broadcasting of personal data does not stop with our leaders, and ‘kompromat’ is not the only risk. Details about everyday Australians are also broadcast, creating personal security risks such as scams and ID theft. This report builds on the ICCL analysis to focus on personal security risks. We are indebted to the ICCL for their analysis.

This report is also a follow-up to our December 2023 report *Australians for Sale*,² which documents the extent to which personal data about Australians is being shared and sold. This report shows it is available to practically anyone, hence the title *Any Buyer Accepted*.

¹ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis* www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

² Reset.Tech 2023 *Australians for Sale* <https://au.reset.tech/uploads/Reset.Tech-Report-Australians-for-Sale-2023.pdf>



Foreword

Foreword from Electronic Frontiers Australia

The personal data of Australians is unknowingly exposed every day, with an on-line system called Real-Time Bidding (RTB), putting our most sensitive data at risk. This foreword serves as a stark warning about the vulnerabilities of RTB and the urgent need for reform.

Imagine: Your location and other attributes about you, where you go and what you do on-line is broadcasted hundreds of times daily to countless unknown companies. This isn't science fiction; it's the chilling reality of RTB where deeply personal details about Australians, including financial health, shopping habits, and even health issues, are constantly broadcasted in a digital free-for-all auction, to bombard you with precisely targeted ads when on-line. All without your knowledge and express consent.

This lack of control over our data also exposes us to a multitude of threats including precisely targeted scams, e.g. fake road toll message and highly effective misinformation and disinformation crafted by both domestic and foreign actors, e.g. deliberately false characterisations about legitimate government policy leading up to an election.

The Problem Goes Beyond Individual Control

While we may use secure devices, RTB goes beyond personal safeguards. The data trail we leave behind extends to our friends, family, and every website we visit. This creates a web of vulnerability that's impossible to manage alone. To fix this problem we need systemic reform, not individual vigilance.

Time for a *Privacy Act* Overhaul

Australia's current *Privacy Act* simply doesn't have the teeth to tackle the invasive nature of RTB, which is only one part of the exploitative surveillance based environment that government and business call "the digital economy".

In past years, privacy and technology observers would say we, as individuals, are the “product” of the digital economy but in reality, sadly, we are really its fuel source. We urgently need stronger regulations that limit the unauthorised collection, sharing, sale, and use of our personal data to prohibit RTB and to shine the light on the hidden ‘surveillance economy’.

RTB and more broadly, online tracking for commercial purposes, dehumanises us through inappropriate and pervasive surveillance, behavioural manipulation, commodification, removal of agency, all of which can result in discrimination and numerous types of harm.

Reforming the *Privacy Act* is therefore crucial to protect Australians from not only being unwittingly exploited by both domestic and foreign actors but from the intrusive and invasive mechanics of the on-line tracking and marketing industry itself.

The Right to Privacy is Fundamental

Our right to privacy is not a luxury; it is a fundamental human right and essential for a secure and democratic society. The RTB system undermines this fundamental right by turning our personal details into a lucrative commodity. We cannot continue to remain blind to how Big Tech exploit our personal data for their profits. Nor can we continue to remain silent.

Let’s raise awareness, demand reform, and ensure our personal data and our privacy is protected against unfair, unreasonable and illegitimate incursions into our on-line lives. We must act together to ensure that our online lives are not exploited, and that our right to privacy is no longer an illusion in the digital age.

John Pane

Chair

Electronic Frontiers Australia

www.efa.org.au



Foreword from Consumer Policy Research Centre

More businesses are using more of our data in more ways than ever before. It can shape what a person sees online, what they're offered, the price they're offered and what they're excluded from. In a more data-driven world than ever before, protecting how personal information is collected, shared and used has never been more important than now.

The biggest boon touted in the digital economy is choice. The choice for what we want, when we want it and how we want it. However, is this choice genuine or is it just a myth?

While new technology offers choice and convenience, without proper protections it can come at a cost to Australians – and often it's with their data.

This research from Reset highlights how little control Australians have over their privacy, yet our current privacy framework disproportionately places on Australians the burden of their own safety online.

There's a power imbalance between industry and us as individuals. They know so much about us and we know so little about how they know what they know. Most of our privacy protections are based on notification and consent. The only way out often is to not use any products or services that play in this game but that leaves Australians with very little options. There isn't a genuine choice.

When it comes to being monitored online or their data being shared with third parties, Australians are rightfully wary. Consumer Policy Research Centre's (CPRC) found that 72% feel they have little to no control over what information is collected from businesses they have no direct contact with.³ While 70% of Australians are not comfortable with companies monitoring their behaviour online, it is happening daily, hourly, almost every second of their lives.⁴ It is not just about the companies that an individual may come into direct contact with, but it is the ecosystem of third-party companies, the names of which many will have never heard of, that have copious amounts of data on us as individuals, singling them out from the crowd.

Australians deserve privacy protections that are centred around people, not profit. It is time for the Federal Government to modernise what it means to be identifiable to cover data points obtained from any source and by any means. It must put the onus on businesses by imposing clear obligations on collecting, sharing and using consumer data that leads to fair and safe outcomes for Australians. To ensure that businesses are held accountable to stronger privacy obligations, the Federal Government must empower regulators to swiftly ban or restrict harmful practices that cause direct and clear consumer harms.

If we want Australians to fully realise the benefits of the digital economy, we need protections that ensure people's safety is placed at its centre. They deserve a digital experience that's fair, safe and meaningful today and in the future.

Chandni Gupta

Deputy CEO and Digital Policy Director

Consumer Policy Research Centre

<https://cprc.org.au/>



³ CPRC 2024, *Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them*, <https://cprc.org.au/report/singled-out>.

⁴ CPRC 2023, *Not a Fair Trade – Consumer views on how businesses use their data*, <https://cprc.org.au/report/not-a-fair-trade-consumer-views-on-how-businesses-use-their-data/>.

Contents

Sensitive data about Australians is widely broadcast without controls via ‘Real-Time Bidding’	11
<i>What is real-time bidding?</i>	12
<i>How much data is shared?</i>	12
<i>What sorts of data are shared?</i>	13
<i>Who can see this data?</i>	15
Scammers and nefarious actors can access this data	16
<i>Toll booth and parcel scams</i>	18
<i>What sorts of data might make us vulnerable to other scam</i>	20
Foreign state actors also have access to this data	25
Conclusions & recommendations	27



1. Sensitive data about Australians is widely broadcast without controls via 'Real-Time Bidding'

1. Sensitive data about Australians is widely broadcast without controls via ‘Real-Time Bidding’

Sensitive data about Australians is broadcast via the Real-Time Bidding (RTB) process to thousands of companies, hundreds of times a day. There is no way to limit or track the spread of RTB data after it is broadcast.

What is real-time bidding?

Every time you pick up your phone or laptop and load new content on a website or app that contains ads, an RTB auction is instantaneously launched to determine what ads appear in front of you. RTB auctions occur in less than a second, meaning the ads can appear as quickly as the content from the website or app. RTB auctions are run by “ad exchange” companies, like Google. To help decide whose ad-space to bid on “ad exchange” companies automatically broadcast troves of personal data on individuals to potential bidders like advertisers and their representatives (called “demand-side platforms” [DSPs]).

How much data is shared?

The scale of data sharing between ad exchanges and DSPs is huge. Thousands of DSP companies can receive data on every ad slot that becomes available on Australians’ phones or websites.⁵ These companies can also copy this data and build their own datasets about Australians.

The amount of data about each Australian that is shared by ad exchanges is massive. On average, **the RTB system broadcasts where a person in Australia is 449 times a day.**⁶ Australians’ data is broadcast this way 3.7 trillion times a year by the online advertising industry (excluding Amazon and Meta, for which we have no data). One dataset alone — the Eyeota (Dun & Bradstreet) dataset — shows 17,501 unique data categories that are for sale about Australians.⁷

⁵ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 5
www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf



⁶ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 7
www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

⁷ Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

- Google’s documentation reports that 2,051 entities may receive data from Google auctions in Australia.⁸
- Microsoft has said that 1,647 firms may receive its RTB data from its auctions. Meta, Amazon and others undoubtedly do the same.⁹
- Google operates the largest RTB system. Google’s RTB system is live on 15.6 million websites and millions of apps, and broadcasts data such as what people are viewing or doing on a website or app and their “hyperlocal” locations, 31 billion times a day, every day in Australia.¹⁰

What sorts of data are shared?

The type of data shared is especially concerning. RTB data broadcasts reveal highly sensitive information about Australians including location and movements over time, sexual interests, financial concerns, banking and utility providers, personal problems, gambling or drinking habits, and recent online purchases.¹¹

 Information	 Source
If you buy condoms	Eyeota Powered by Ibotta - Purchasers - Primary Category - Sexual Health (Users who have purchased items of Sexual Health category) ¹² Eyeota Powered by Ibotta - Purchasers - Sexual Health - Family Planning (Users who have purchased Family Planning) ¹³
If you overeat to cope with stress	AU RDA Research - Lifestyle - Indulgent Consumption (Indulging yourself with luxuries, new purchases & treats) ¹⁴

⁸ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 6 www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

⁹ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 6 www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

¹⁰ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 7 www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

¹¹ See generally, Reset.Tech 2023 *Australians for Sale* <https://au.reset.tech/uploads/Reset.Tech-Report-Australians-for-Sale-2023.pdf>

¹² Row 6,592 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

¹³ Row 17,457 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

¹⁴ Row 10,664 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

 Information	 Source
	<p><i>'Loving the thrill of buying new things & acting on impulse without thinking too deeply. Also being luxuriously self indulgent whenever one gets the chance & over-eating to cope with stress. Based on modelled offline data.'</i></p>
<p>If you're interested in intelligence and counter terrorism</p>	<p>Global ShareThis - Law and Government - Government - Intelligence and Counterterrorism¹⁵</p> <p><i>'Consumers with recent interest in intelligence and counterterrorism; observed from social sharing, searched page visits and click-backs on shared pages.'</i></p>
<p>If you're worried about cholesterol</p>	<p>AU Nielsen CMV - Health & Fitness - Lifestyle - Concerned about my cholesterol level¹⁶</p> <p><i>'More likely to have the opinion about Health ,I am concerned about my cholesterol level' based on modelled offline data'</i></p>
<p>If you're a mother</p>	<p>Eyeota - AU - Demo - Family - Parents - Mothers Eyeota Users who are Mothers based on declared or registered information¹⁷</p>
<p>If you actively gamble</p>	<p>'Users who Gamble' Eyeota - AU - Lifestyle - Intent - Gambling¹⁸</p> <p>(Note this is <i>intent</i> to gamble, which is one step further than an <i>'interest in'</i> gambling)</p>
<p>If you worry about your weight</p>	<p>'Diet and Weight loss' Eyeota - AU - Health and Fitness - Interest - Diet and Weight Loss¹⁹</p> <p><i>'Users who browse content such as articles, reviews and blog posts that demonstrate an interest in Health and Fitness, specifically Diet and Weight Loss'</i></p>

¹⁵ Row 15,394 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

¹⁶ Row 6,522 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

¹⁷ Row 550 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

¹⁸ Row 439 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

¹⁹ Row 417 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

 Information	 Source
Whether you prefer Fanta or Sprite	AU Nielsen CMV - CPG & FMCG - Intent - Carbonated Drinks - Sprite (More likely to drink Sprite, based on modelled offline data) ²⁰ AU Nielsen CMV - CPG & FMCG - Intent - Carbonated Drinks - Fanta (More likely to drink Fanta, based on modelled offline data) ²¹
Right down to whether you buy Knorr stock cubes	Global Affinity Answers - Intent - Pasta - Knorr. This segment identifies shoppers most likely to purchase Knorr products ²²
Or whether you got your vacuum from Godfreys	HYP PTY LTD 12281 25082765 Godfreys (location) ²³

Who can see this data?

The sale of a single ad slot often involves an ‘auction of auctions’, with several ad exchanges running competing auctions that serve to increase the number of DSP companies that receive the data.

However, the data is broadcast without adequate security measures.²⁴ After the broadcast, there is no way to track or limit how receiving entities handle the RTB data; nor is there any technical method to stop further distribution of RTB data. Industry documentation confirms “there is no technical way to limit the way data is used” after broadcast.²⁵

²⁰ Row 1,181 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

²¹ Row 1,187 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

²² Row 3,154 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

²³ Row 589174 Irish Council of Civil Liberties 2024 *Microsoft Xandr Data Marketplace RTB Segment List* (global, including Australia), May 2021 www.iccl.ie/wp-content/uploads/2023/10/Doc-1-Xandr-Data-Marketplace-May-2021.pdf

²⁴ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 6 www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

²⁵ IAB Europe and IAB Tech Lab 2018 *GDPR Commit Group Publishers concerns about IAB’s GDPR Transparency & Consent Framework version 1.1* www.github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#liability



2. Scammers and nefarious actors can access this data

2. Scammers and nefarious actors can access this data

Because there are no effective limits on who can see all this sensitive information, it is accessible to scammers and other nefarious actors. Many of the datasets that are made available would serve to target scams extremely effectively.

A huge number of entities receive extraordinarily sensitive RTB data about Australians, and there is no way to control what they then do with the data. In other words, there is no way to stop data shared in the RTB process from being re-shared or reused by other actors. In effect, there is no real method to know who the data is shared with. This creates an enormous free-for-all of very sensitive data about everyday Australians. It is already known that there are companies gathering data from the RTB process to repackage and sell.²⁶

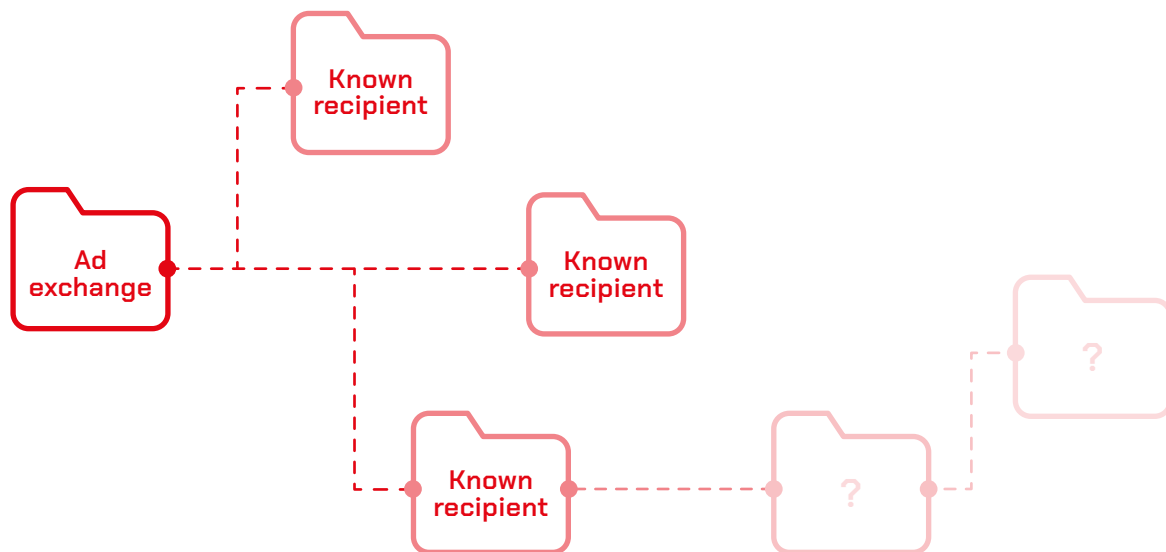


Figure 1: A diagram showing how data can flow from an ad-exchange to known DSP recipients, but then the flow of this data is untraceable

This means that data gathered about Australians ostensibly for the purpose of delivering ‘targeted advertising’ can also be purchased by those wishing to deliver ‘targeted scams’.

²⁶ Irish Council of Civil Liberties 2024 *Australia’s hidden security crisis*, pg. 8 www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

Part of the reason scams have become an increasing issue over the last decade is how deeply deceptive and accurate they have become. This is particularly true for impersonation scams, such as bank scams, utility provider scams, parcel delivery scams, and tollway scams, where scammers contact victims and pretend to be from their bank or another legitimate company. One reason people are vulnerable to these scams is that scammers often possess extensive information about their victims, creating an illusion of legitimacy.

For instance, in its consumer guidance on identifying scams, the Australian Communications and Media Authority advises that one way to be a scam target is if ‘someone you don’t know has your personal details. A scammer might have stolen your personal details and used them to convince you they are a trusted business (for example, pretending to be your bank or telco provider)’.²⁷ While some scammers may have indeed stolen this data or accessed it through data breaches, this is a comparatively circuitous and inefficient route. Data about people’s banking providers and habits are widely and easily accessible via the RTB system.

The exact playbook scammers use is known only to the scammers themselves. However, data about potential victims is key to scamming networks, and much of the data made available about Australians via the RTB process creates vulnerabilities. It is unclear why scammers would rely on incomplete, harder-to-access stolen data sources to personalise scams, when the RTB system is a comparatively accessible market and a (currently) legal trade.

Toll booth and parcel scams

Two particularly widespread scams in Australia are fake toll booth scams and fake parcel delivery scams.

Toll booth scams

Overall, 7 in 10 Australian adults (70%, or 18.2 million) have received a scam message asking them to pay an unpaid road toll.²⁸ Certain data segments that can narrow down who is more likely to incur road toll charges, which scammers could access to make their targeting more precise:

²⁷ ACMA 2024 *How to spot a scam* www.acma.gov.au/phone-and-sms-scams

²⁸ According to an August 2024 YouGov poll, commissioned by Reset.Tech, n=1,039

👁 Insight	📁 Segment	🔍 Observation
Those that are more likely to spend on personal transport (specifically road tolls)	Road Tolls - based survey data AU Digifish - Transport - Intent - Road Tolls ²⁹	Digifish describe themselves as specialising in ‘Real-time people movement linking offline to online customer behaviors, demographics, and spend data’. ³⁰
Those ‘Likely to have increased spend on road tolls’	AU smrtr - Consumer Spending - Transport - Road Tolls ³¹	smrtr describe themselves as using ‘genuine transactional data from industry partners’, as well as mobile handset data covering ‘50 billion location pings’ per year. ³²

Parcel scams

Overall, 8 in 10 Australian adults (precisely 81%, or 21 million) have received a parcel delivery scam message, including those from scammers pretending to be Australia Post.³³ If a scammer wants to know whether you are expecting a parcel to be delivered and are thus susceptible to an ‘Australia Post delivery fee’ scam message, there are data segments for sale that specifically identify who is expecting parcels, for example:

👁 Insight	📁 Segment
Consumers with recent interest in mail and package delivery; observed from social sharing, searched page visits and click-backs on shared pages	Global ShareThis - Business and Industrial - Transportation and Logistics - Mail and Package Delivery ³⁴

²⁹ Row 8,633 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

³⁰ DigiFish nd LinkedIn Profile www.linkedin.com/company/digifish-group/ archived at www.web.archive.org/web/20240902030643/https://www.linkedin.com/company/digifish-group/

³¹ Row 10,235 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

³² smrtr nd Data Universe www.smrtr.com.au/data-universe/ archived at www.web.archive.org/web/20240902091255/https://smrtr.com.au/data-universe

³³ According to an August 2024 YouGov poll, commissioned by Reset.Tech, n=1,039




³⁴ Row 15,597 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

We asked Cherie Clonan, an experienced advertising executive, if they felt there were ‘legitimate’ uses justifying the use of the trade in data segments about toll booths and parcel deliveries. They said:

“In 10 years of CEO’ing The Digital Picnic and close to 20+ years within this industry as a whole, I’ve never seen a legitimate use for this sort of data.”

What sorts of data might make us vulnerable to other scams?

If a scammer wants to know whether you’ve recently arrived in the country or travelled, which could make you vulnerable to a scam message from border control saying you have ‘urgent visa issues’, there are data segments that identify people who have recently travelled through international airports:

 Insight	 Segment	 Observation
Devices seen at low cost airport terminals in the last 90 days	Global Lifesight - Travel - Location Visited - Low Cost Airports ³⁵	This appears to be geo-located data.
Devices seen at airports in the last 90 days	Global Lifesight - Transport - Location Visited - Airports ³⁶	This appears to be geo-located data.
Devices seen <i>frequently</i> at airports in the last 90 days	Global Lifesight - Travel - Location Visited - Frequently at Airports ³⁷	This appears to be geo-located data.

If a scammer wants to know who you bank with, so they can personalise a banking scam, there are data segments that identify customers of various banks:

³⁵ Row 11,924 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

³⁶ Row 11,933 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

³⁷ Row 11,925 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

 Bank	 Segment
Westpac	Global Lifesight - Finance - Location Visited - Westpac Lifesight - Devices seen at Westpac in the last 90 days ³⁸ AU Nielsen CMV - Finance - Product Ownership - Banking - Main Institution - Westpac Nielsen CMV More likely to have Westpac as their main financial institution (MFI), based on modelled offline data ³⁹ AU Digifish - Finance - Intent - Brand - Westpac Digifish Those with a high index which have visited, engaged, or purchased the brand in the last 30 days, with above average socioeconomic status (sic) ⁴⁰
NAB	Nielsen CMV - Finance - Product Ownership - Banking - Main Institution - NAB Nielsen CMV More likely to have NAB as their main financial institution (MFI), based on modelled offline data ⁴¹
Suncorp	AU Digifish - Finance - Intent - Brand - Suncorp Digifish Those with a high index which have visited, engaged, or purchased the brand in the last 30 days, with above average socioeconomic status (sic) ⁴²
AMP Bank	Digifish - Finance - Intent - Brand - AMP Bank Digifish Those with a high index which have visited, engaged, or purchased the brand in the last 30 days, with above average socioeconomic status (sic) ⁴³
BankWest	AU Digifish - Finance - Intent - Brand - Bankwest Digifish Those with a high index which have visited, engaged, or purchased the brand in the last 30 days, with above average socioeconomic status (sic) ⁴⁴

³⁸ Row 7,953 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

³⁹ Row 1,030 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf



⁴⁰ Row 7,259 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

⁴¹ Row 1,031 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf



⁴² Row 7,262 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

⁴³ Row 7,283 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

⁴⁴ Row 7,278 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

 Bank	 Segment
Commonwealth Bank	AU Digifish - Finance - Intent - Brand - Commonwealth Bank Digifish Those with a high index which have visited, engaged, or purchased the brand in the last 30 days, with above average socioeconomic status (sic) ⁴⁵
Macquarie Bank	AU Digifish - Finance - Intent - Brand - Macquarie Bank Digifish Those with a high index which have visited, engaged, or purchased the brand in the last 30 days, with above average socioeconomic status (sic) ⁴⁶
Adelaide Bank	Branded Data - Lifesight - Brand Shoppers - Australia - Financial - Adelaide Bank (BlueKai) ⁴⁷
Allianz	Branded Data - Lifesight - Brand Shoppers - Australia - Financial - Allianz (BlueKai) ⁴⁸

If a scammer wants to know who provides your telephone service, so they can personalise a telco scam, there are data segments that identify customers of various telco providers:

 Telco	 Segment
Vodafone	Market research on Mobile Internet Service Provider (AU Experian - Owned - Personal Mobile Service Provider - Vodafone) ⁴⁹
Virgin	Market research on Mobile Internet Service Provider (AU Experian - Owned - Personal Mobile Service Provider - Virgin) ⁵⁰

⁴⁵ Row 7,273 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

⁴⁶ Row 7,269 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

⁴⁷ Row 374340 Irish Council of Civil Liberties 2024 Microsoft Xandr Data Marketplace RTB Segment List (global, including Australia), May 2021 www.iccl.ie/wp-content/uploads/2023/10/Doc-1-Xandr-Data-Marketplace-May-2021.pdf



⁴⁸ Row 374341 Irish Council of Civil Liberties 2024 Microsoft Xandr Data Marketplace RTB Segment List (global, including Australia), May 2021 www.iccl.ie/wp-content/uploads/2023/10/Doc-1-Xandr-Data-Marketplace-May-2021.pdf

⁴⁹ Row 6,016 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

⁵⁰ Row 6,017 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Bradstreet-Eyeota-July2024.pdf

 Telco	 Segment
Virgin	Market research on Mobile Internet Service Provider (AU Experian - Owned - Personal Mobile Service Provider - Telstra) ⁵¹ People who have visited Telstra 'locations', presumably shops: HYP PTY LTD 12281 25082781 Telstra (location)) ⁵²
Optus	Market research on Mobile Internet Service Provider (AU Experian - Owned - Personal Mobile Service Provider - Optus) ⁵³ People who have visited Optus 'locations' presumably shops: (HYP PTY LTD 12281 25082780 Optus (location)) ⁵⁴

If a scammer wants to know if you've recently bought concert tickets, so they can personalise a ticket scam, there are data segments that identify who has recently purchased tickets:

 Insight	 Segment
People who have purchased concert tickets in the last month	Internet Purchase Types in the month prior to survey response – AU Experian - Past Purchased - Purchased Online Past Month - Concert/Event Tickets ⁵⁵
Users who browse content such as articles, reviews and blog posts that demonstrate an interest in Events, specifically Concerts	Eyeota - AU - Entertainment - Interest - Events - Concerts ⁵⁶

⁵¹ Row 6,018 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

⁵² Row 589187 Irish Council of Civil Liberties 2024 Microsoft Xandr Data Marketplace RTB Segment List (global, including Australia), May 2021 www.iccl.ie/wp-content/uploads/2023/10/Doc-1-Xandr-Data-Marketplace-May-2021.pdf

⁵³ Row 6,020 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

⁵⁴ Row 589186 Irish Council of Civil Liberties 2024 Microsoft Xandr Data Marketplace RTB Segment List (global, including Australia), May 2021 www.iccl.ie/wp-content/uploads/2023/10/Doc-1-Xandr-Data-Marketplace-May-2021.pdf

⁵⁵ Row 5,813 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

⁵⁶ Row 502 Irish Council of Civil Liberties 2024 Eyeota (Dun & Bradstreet) Segments On Australians (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf

🎯 Insight	📁 Segment
People who have demonstrated intent to buy entertainment	Eyeota - AU - Entertainment - Intent - Users who have demonstrated an intent to buy through actions like product searches, configurations and comparisons for Entertainment products ⁵⁷

All of the data made available through the RTB process leaves us vulnerable to scammers and nefarious actors.

⁵⁷ Row 512 Irish Council of Civil Liberties 2024 *Eyeota (Dun & Bradstreet) Segments On Australians* (Obtained by ICCL Enforce in July 2024) www.iccl.ie/wp-content/uploads/2024/07/Doc-3-Australia-Dun-and-Brandstreet-Eyeota-July2024.pdf



3. Foreign state actors also have access to this data

3. Foreign state actors also have access to this data

Foreign states and non-state actors can easily obtain sensitive data about Australians via the RTB system. Laws in Russia and China require domestic firms – such as those registered as advertisers and their representatives – to share this data with the state if they request it.

The RTB system provides both Chinese and Russian state actors with a secure pipeline to access data about everyday Australians if they want it. Any DSP company (advertisers or their representative) in China that has RTB data about Australians can be compelled to share it with the Chinese government. The 2021 Data Security Law of the People's Republic of China allows Chinese state actors to access Australian RTB data once it is in the hands of Chinese companies. Likewise, any Russian companies can be compelled to share their data with the Russian government, as Russian law allows security services to access any data collected by companies on Russian soil.

We know that:

- Google sends Australia RTB data to many companies in China. Before sanctions were enacted, Google also sent Australia RTB data to Russian companies.⁵⁸ It is unclear whether this practice would recommence if sanctions were lifted. Russian companies that Google sent Australia RTB data to include AiData, which sells profiles on Russians who visit Russian political opposition websites.⁵⁹
- Microsoft's RTB firm Xandr also sends Australian RTB data to Chinese entities. It previously sent it to Russian entities as well.⁶⁰

⁵⁸ Irish Council of Civil Liberties 2024 *Australia's hidden security crisis*, pg. 7
www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

⁵⁹ Irish Council of Civil Liberties 2024 *Australia's hidden security crisis*, pg. 7
www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf

⁶⁰ Irish Council of Civil Liberties 2024 *Australia's hidden security crisis*, pg. 7
www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf



4. Conclusions & recommendations

Conclusions & recommendations

Sensitive data about Australians is broadcast via RTB to many entities, hundreds of times a day. There is no way to limit or track the spread of RTB data after they are broadcast.

Because there are no effective limits on who can access this sensitive information, it is available to scammers and other nefarious actors. Many of the datasets made available could serve to direct scams at vulnerable targets extremely effectively. We do not know all the methods by which scammers target Australian victims, and many may use a ‘scatter gun’ approach; however, the free flow of data making Australians vulnerable to targeted scams creates unnecessary risk.

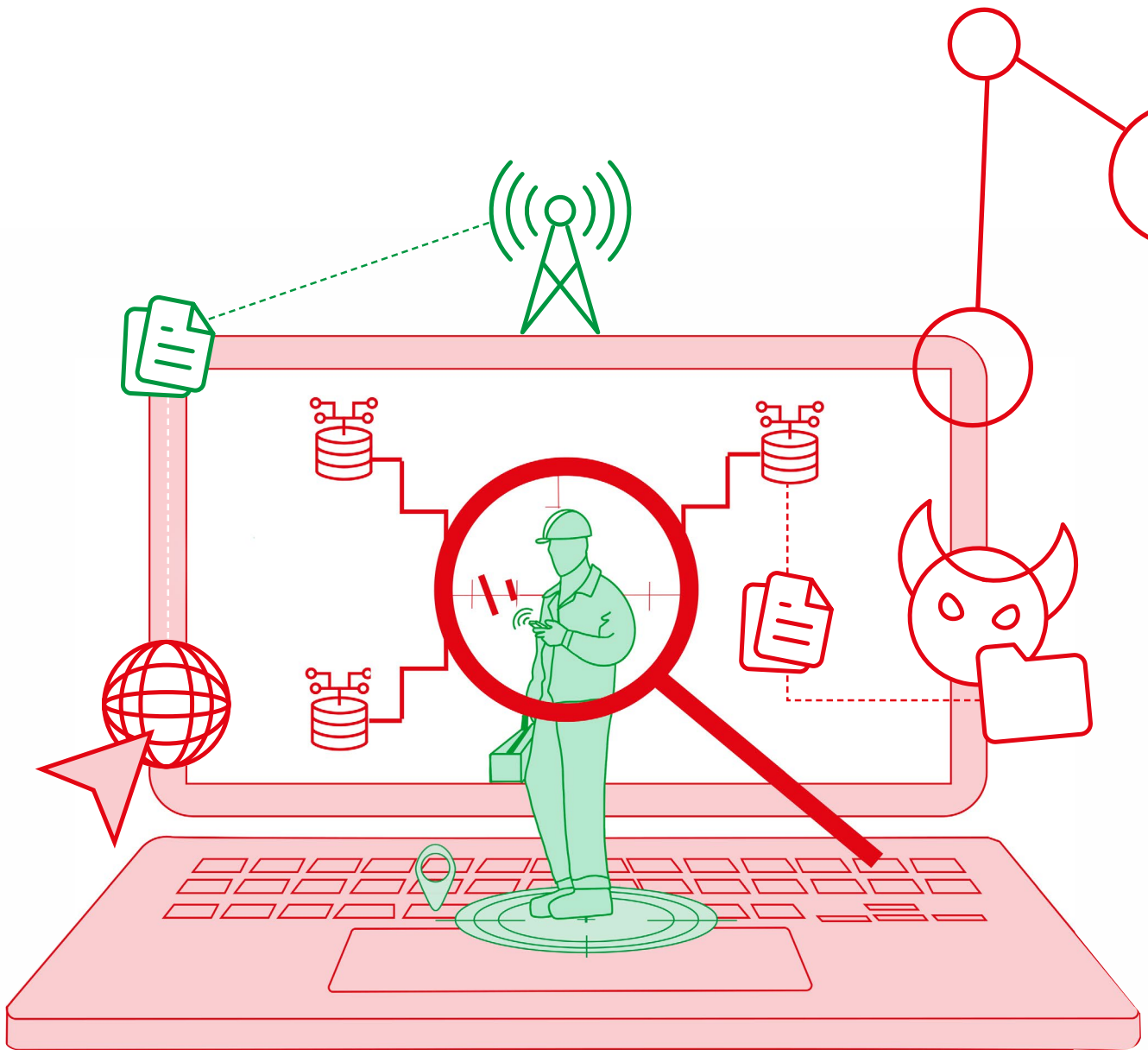
Further, foreign states and non-state actors can easily obtain Australians’ sensitive data easily via the RTB system. Laws in Russia and China require domestic firms – such as those registered as advertisers and their representatives – to share this data with the state if they request it.

These risks are beyond the control of individuals to manage. Even if we use secure devices, data will still flow via RTB from personal devices as well as devices of friends, family, and personal contacts. Overall, stronger data protections to regulate the flow of this information are required.

We note key elements in the Government’s regulatory pipeline are relevant – namely the Scams Prevention Framework and the statutory review of the *Online Safety Act 2021*. These valuable, necessary interventions do not account for the creation and marketisation of personal data that creates foreseeable personal security risks. Proactive obligations need to be placed on data collecting and data trading firms to exercise fairness and reasonableness in the collection of personal data.

To address this, Australia urgently needs effective privacy protections. The protections detailed in the *Privacy Act Review*⁶¹ are an excellent starting point for protecting Australians’ data. Australians cannot afford to wait any longer for *Privacy Act* reform.

⁶¹ Attorney General’s Department 2023 *Government response to the Privacy Act Review Report*
www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report



Reset·Tech

AUSTRALIA

Any Buyer Accepted

Unregulated data markets create personal security risks, including scams and foreign interference

October 2024

<https://au.reset.tech/>



CC BY 4.0 DEED

Attribution 4.0 International